



# Department of Homeland Security Daily Open Source Infrastructure Report for 14 December 2005

Current  
Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

## Daily Highlights

- The Associated Press reports a federal judge has lifted the final legal barrier to completing a border fence meant to thwart illegal immigrants in the southwestern corner of the U.S. (See item [12](#))
- Health-IT World reports public health experts preparing for a feared avian flu pandemic are using computer models to get an idea of how the disease might spread if the bird virus were to start passing between people. (See item [22](#))

## DHS Daily Open Source Infrastructure Report *Fast Jump*

**Production Industries:** [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

**Service Industries:** [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

**Sustenance and Health:** [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

**Federal and State:** [Government](#); [Emergency Services](#)

**IT and Cyber:** [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

**Other:** [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *December 13, United Press International* — **ConocoPhillips pays \$35.6B for natural gas.** ConocoPhillips, the third largest U.S. energy company, is paying \$35.6 billion to increase its access to North American natural gas. The cash-and-stock deal for Houston's Burlington Resources Inc. gives ConocoPhillips, also Houston-based, long-term natural gas reserves at a time when the commodity and the demand for it has reached record levels. The transaction also enhances ConocoPhillips production growth and North American gas supply position both in the near term, through projects involving conventional and unconventional resources, and in the long term through liquefied natural gas and Arctic gas projects.

Source: [http://www.industrywatch.com/pages/iw/customer/Story.nsp?story\\_id=86686532&ID=iw&scategory=Energy%3ANatural+Gas&](http://www.industrywatch.com/pages/iw/customer/Story.nsp?story_id=86686532&ID=iw&scategory=Energy%3ANatural+Gas&)

2. *December 13, Agence France–Presse* — **Asean eyes renewable power sources.** The strain of soaring oil prices is making Asian nations take a look at everything from wind power to coconuts to meet energy needs, but officials and analysts say there are no easy answers ahead. Energy security has been a major topic at the Association of Southeast Asian Nations (Asean) summit, held in Kuala Lumpur this week, with the bloc's political leaders calling for greater cooperation to slash dependence on imported oil. Nuclear energy, geothermal, hydroelectric, and wind power have increased their attractiveness, with oil hitting record levels in August and remaining around \$60 per barrel. Malaysia, the world's biggest producer of palm oil, is pushing to develop bio–fuel from the plant, while the coconut–producing Philippines is offering to host a regional hub for ethanol fuel. But Dave Ernsberger, Asia oil director for energy information giant Platts, said Asean's biggest challenge was how to deal with the destabilizing effect of Indonesia's plunge from being an oil exporter to a net importer.

Source: <http://www.sunstar.com.ph/static/ceb/2005/12/14/bus/asean.eyes.renewable.power.sources.html>

[[Return to top](#)]

## **Chemical Industry and Hazardous Materials Sector**

3. *December 13, Daily Press (VA)* — **Logging, propane trucks collide, prompting road closure in Virginia.** A logging truck caught fire after it rear–ended a propane truck on Holland Road in southern Suffolk, VA, on Monday morning, December 12. A small leak at the propane truck was quickly contained, said Lt. Debbie George of the Suffolk Police Department, but the logging truck was destroyed. Police closed both lanes of Holland Road for about 30 minutes and charged the driver of the logging truck with reckless driving. Both drivers went to Obici Hospital with non–life–threatening injuries.

Source: <http://www.dailypress.com/news/local/dp–37488bf0dec13.0.5193192.story?coll=dp–briefs>

4. *December 13, Associated Press* — **Ruptured gas line causes New Jersey explosion.** Construction workers in Bergenfield, NJ, hit a gas line Tuesday, December 13, and touched off an explosion that tore through a three–story apartment building, causing at least part of it to collapse, authorities said. Six people were injured, said New Jersey Police Capt. Rick McGarril. Law enforcement and utility company officials said preliminary investigations showed that a pit dug by construction workers who were trying to remove an underground oil tank collapsed and pinched a gas line just before 9 a.m. EST. Utility crews were sent to the scene after residents nearby reported the odor of gas; 30 minutes later, the explosion shook the area. Hackensack University Medical Center treated three people from the explosion, said hospital spokesperson Lesley Bruno. The explosion sent up plumes of smoke that could be seen more than 10 miles away. Firefighters evacuated several nearby homes in case the fire spread. Bergenfield, with a population of 26,000, is located six miles northwest of New York City.

Source: <http://www.nj.com/newsflash/national/index.ssf?/base/national–56/1134488350314730.xml&storylist=national>

5. *December 12, Associated Press* — **Thousands of gallons of heating oil spilled after tanker accident in New Jersey.** Thousands of gallons of heating oil spilled onto area streets Sunday afternoon, December 11, after a car and a tanker truck collided, causing the tanker to crash into a closed hamburger stand on the border of Pennsauken and Camden, NJ. The accident, which occurred around 3:45 p.m. EST on Route 130–South near Federal Street, forced officials to shut down a stretch of the roadway for several hours. Fumes from the spill also spurred officials to evacuate about 30 people from a nearby apartment complex as a precaution. Many residents were taken to a nearby shelter and had not returned home by late Sunday night. About 8,000 gallons was spilled, including a large portion that made its way into nearby sewers, but officials said they did not believe the spill would reach area rivers or pose any major health or environmental problems.  
Source: <http://www.wnbc.com/traffic/5516327/detail.html>

[[Return to top](#)]

## **Defense Industrial Base Sector**

6. *December 13, Government Accountability Office* — **GAO–06–49: Unmanned Aircraft Systems: DoD Needs to More Effectively Promote Interoperability and Improve Performance Assessments (Report).** Unmanned aircraft systems (UAS) consist of an unmanned aircraft; sensor, communications, or weapons, carried on board the aircraft, collectively referred to as payloads; and ground controls. UAS have been used successfully in recent operations, and are in increasingly high demand by U.S. forces. To meet the demand, the Department of Defense (DoD) is increasing its investment in and reliance on UAS, and often deploying them while still in development. The Government Accountability Office (GAO) has previously found that DoD's approach to developing and fielding UAS risked interoperability problems, which could undermine joint operations. GAO was asked to review (1) UAS performance in recent joint operations and (2) the soundness of DoD's approach to evaluating joint UAS operational performance. GAO recommends that the Secretary of Defense develop and apply appropriate joint operating standards, and include specific performance indicators and baselines for analysis and systematic information reporting and analysis procedures in the new performance measurement system under development. In commenting on a draft of this report, DoD fully or partially concurred with GAO's recommendations.  
Highlights: <http://www.gao.gov/highlights/d0649high.pdf>  
Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-49>

[[Return to top](#)]

## **Banking and Finance Sector**

7. *December 13, Government Technology* — **In big data breaches, few identities misused for criminal financial gain.** Last week, ID Analytics Inc., an identity risk management company, announced findings from its analysis of four data breaches involving approximately half a million consumer identities. A significant finding from the research is that different breaches pose different degrees of risk. In the research, ID Analytics distinguishes between "identity-level" breaches, where names and Social Security numbers were stolen and

"account-level" breaches, where only account numbers were stolen. ID Analytics also discovered that the degree of risk varies based on the nature of the data breach, for example, whether the breach was the result of a deliberate hacking into a database or a seemingly unintentional loss of data. The research makes it clear that identity-level breaches pose the greatest potential for harm to businesses and consumers due to fraudsters' sophisticated methods for profiting from identity information, as compared to account-level breaches. Even so, the calculated fraudulent misuse rate for consumer victims of the analyzed breach with the highest rate of misuse was 0.098 percent — less than one in 1,000 identities. Another key finding indicates that in certain targeted data breaches, notices may have a deterrent effect. In one large-scale identity-level breach, thieves slowed their use of the data to commit identity theft after public notification.

Source: <http://www.govtech.net/news/news.php?id=97547>

**8. *December 12, Computer World* — Security breach at Sam's Club exposes credit card data.**

Sam's Club, a division of Wal-Mart Stores Inc., is investigating a security breach that has exposed credit card data belonging to an unspecified number of customers who purchased gas at the wholesaler's stations between September 21 and October 2. In a brief statement released December 2, the Bentonville, AR-based company said it was alerted to the problem by credit card issuers who reported that customers were complaining of fraudulent charges on their statements. It's still not clear how the data was obtained, according to the statement. But "electronic systems and databases used inside its stores and for Samsclub.com are not involved," the company said. Sam's Club is currently working with both Visa International Inc. and MasterCard International Inc. to investigate the breach. The company also has notified the U.S. Attorney's Office for the Western District of Arkansas and the U.S. Secret Service. In a statement, Visa said it has alerted all of the affected financial institutions, asked them to provide independent fraud-monitoring services to affected customers and requested that they issue new cards as needed.

Source: <http://www.computerworld.com/securitytopics/security/story/0,10801,107014,00.html>

[\[Return to top\]](#)

## **Transportation and Border Security Sector**

**9. *December 13, Associated Press* — Congress turns attention to cruise safety. A**

Congressional subcommittee that is primarily focused on terrorism is turning its attention to threats lurking on the high seas amid peaceful vacations. The Subcommittee on National Security, Emerging Threats and International Relations and another subcommittee had a joint hearing Tuesday, December 13, in Washington, DC, focusing on cruise ship disappearances and crimes. The hearing came after about a dozen disappearances of cruise ship passengers in recent years. In the latest case, George Allen Smith IV of Greenwich vanished July 5 from a Royal Caribbean ship in the Mediterranean between Greece and Turkey. The FBI has been investigating, but no one has been charged and no body has been recovered. "We want to know how often this kind of thing happens," said U.S. Rep. Christopher Shays (R-CT), co-chairman of the national security subcommittee. "We've never really looked at cruise ships in terms of public safety." Shays said he wants to know how such incidents are investigated and how authorities determine jurisdiction in international waters. The congressional hearing, "International Maritime Security," included testimony from cruise ship officials about their

procedures for responding to incidents and jurisdictional conflicts related to investigations. The issue has been a concern in the past.

Source: [http://www.usatoday.com/travel/news/2005-12-13-cruise-safety\\_x.htm](http://www.usatoday.com/travel/news/2005-12-13-cruise-safety_x.htm)

10. *December 13, Houston Chronicle* — **Suspicious odor prompts evacuation of Continental flight.** Crewmembers on a Continental Airlines flight noticed a suspicious odor on Monday, December 12, about 6 p.m. CST, when Flight 1425 from Mexico City touched down at Houston's Bush Intercontinental Airport, prompting an evacuation of the passengers. The 94 passengers on the 737 used the emergency slides to leave the aircraft, Continental Airline officials said. The source of the odor is under investigation.

Source: <http://www.chron.com/disp/story.mpl/metropolitan/3520560.htm> 1

11. *December 13, Canadian Press* — **Canadian port gets first radiation detector in bid to thwart nuclear terror.** Federal officials have installed Canada's first radiation detector at the port of Saint John in New Brunswick, in a bid to protect the country against nuclear terrorism. The Canadian Press has learned that while Saint John, New Brunswick, is the first port to get the nuclear detection devices, all major Canadian ports soon will be equipped with the anti-terrorism technology. "It is the first port in Canada to have the equipment up and running," Jennifer Morrison of the Canada Border Services Agency said Tuesday, December 13. The radiation detection program is a key part of Ottawa's \$172-million plan to beef up marine security — all stemming from the terrorist attacks in the United States on September 11, 2001. The devices, which have been in use for two weeks in Saint John, detect radiation inside containers. Yet, critics warn it is still not enough protection in an increasingly dangerous world. Douglas Ross, a professor of political science at Simon Fraser University and an expert in the terrorist threat to North America, said Canada needs a more expensive, double-barreled protection system, employing not only radiation detection equipment but also X-rays that can reveal possible mysterious dark spaces inside containers.

Source: <http://www.940news.com/nouvelles.php?cat=23&id=121331>

12. *December 13, Associated Press* — **Judge approves stretch of San Diego's border fence.** A federal judge has lifted the final legal barrier to completing a border fence meant to thwart illegal immigrants in the southwestern corner of the U.S. The project comprises 14 miles of additional fencing in San Diego. Litigation has stalled the project since it was approved by Congress in 1996. U.S. District Judge Larry Burns said Congress delegated such authority to Department of Homeland Security Secretary Michael Chertoff in June, and noted on Monday, December 12, that the executive branch already had significant jurisdiction over national security and immigration. The final leg of the fence would cross steep, rugged canyons including "Smuggler's Gulch," a maze of trails once overrun by illegal border crossers.

Source: [http://www.abqtrib.com/albq/nw\\_national/article/0.2564.ALBO\\_19860\\_4311546.00.html](http://www.abqtrib.com/albq/nw_national/article/0.2564.ALBO_19860_4311546.00.html)

13. *December 13, Associated Press* — **NYC adopts transit strike contingency plan.** New York City has issued contingency plans in the event of a transit strike that call for cars entering the busiest areas of Manhattan to carry at least four people and public schools to open two hours later than usual. Subway and bus workers voted over the weekend to give the Transport Workers Union board the power to call a strike at 12:01 a.m. EST Friday, December 16, if necessary. On Tuesday, December 13, a judge heard arguments by lawyers for the Metropolitan



Transportation Authority hoping for an injunction to avert a strike. Metro–North Railroad and the Long Island Rail Road commuter lines also have released contingency plans. The city also said yellow taxis would be allowed to carry multiple fares during a strike. The Port Authority of New York and New Jersey said it planned to run PATH trains from the World Trade Center to 33rd Street in midtown. The comptroller's office has estimated that a strike would cost the city more than \$200 million per day in lost economic activity and productivity.

Source: <http://www.wnyc.org/news/articles/54973>

**14. *December 12, USA TODAY* — TSA chief tells Congress bombs are main threat to planes.**

The nation's aviation security chief said Monday, December 12, that airplanes are no longer vulnerable to being hijacked but could be blown up with bombs smuggled into the passenger cabin. Transportation Security Administration (TSA) chief Kip Hawley testified at a Capitol Hill hearing that security improvements since the September 11, 2001, attacks have made hijacking virtually impossible. Hawley cited improvements that include disrupting terrorist cells, hardening cockpit doors, and hiring thousands of air marshals to ride undercover on flights. "It's not about scissors, it's about bombs," Hawley said. The new policy allows scissors with blades up to four inches and tools such as screwdrivers and pliers measuring up to seven inches. Hammers, saws and other sharp tools will remain banned. Screeners recently got extra training in detecting bombs and bomb components, Hawley said.

Source: [http://www.usatoday.com/news/nation/2005-12-12-tsa-hijacking\\_s\\_x.htm](http://www.usatoday.com/news/nation/2005-12-12-tsa-hijacking_s_x.htm)

[[Return to top](#)]

## **Postal and Shipping Sector**

**15. *December 13, Associated Press* — Strong consumer spending, online shopping help FedEx, UPS.**

A resilient national economy and the continuing popularity of Internet shopping have shipping giants FedEx and United Parcel Service predicting business growth for the holiday season. Memphis–based FedEx Corp. expected its busiest day of the year Monday, December 19, with package deliveries totaling 8.5 million, a five percent increase over last year. Atlanta–based UPS Inc. braced for its peak on December 20 with deliveries of more than 20 million packages, also an increase over last year. Neither company knows for sure how many of those packages are headed to online shoppers, but with a nationwide growth of more than 20 percent a year predicted for Internet sales, many obviously are. "It's just a convenient way to shop," said Jeff Wallace, a University of Memphis economist. Internet shoppers can't simply bring their purchase home. Someone must deliver them.

Source: <http://www.southernstandard.net/news.php?viewStory=26145>

[[Return to top](#)]

## **Agriculture Sector**

**16. *December 13, Associated Press* — Wyoming to trap elk to fight disease.** A trap has been built at a state elk feedground near Pinedale, WY, as part of a pilot program to test elk for brucellosis and slaughter those which test positive. "We're still trying to figure out a few of the little logistical things, but the trap is in and ready," said Brandon Scurlock, a Wyoming Game and

Fish Department habitat biologist. The goal is to see if “test and slaughter” can reduce disease rates among elk which frequent the Muddy Creek feedground near Boulder. Elk in the area are suspected of spreading brucellosis to nearby cattle herds, causing Wyoming to lose its federal brucellosis-free status last year and triggering costly testing requirements for Wyoming cattle headed out of state. The pilot project could later involve the Scab Creek and Fall Creek feedgrounds. Under the proposal, as many as 10 percent of the 1,900 or so elk in the Pinedale herd could be slaughtered each winter, although the Game and Fish Department estimates that only 80 or so animals might be slaughtered in the program's early stages. Game and Fish officials have said that if the program succeeded in lowering exposure and infection rates around Pinedale, other traps could be constructed on more feedgrounds.

Source: <http://www.billingsgazette.com/index.php?tl=1&display=rednews/2005/12/13/build/wyoming/25-elk-trap.inc>

[\[Return to top\]](#)

## **Food Sector**

17. *December 13, Associated Press* — **Japan supermarkets cautious of U.S. beef.** Japan's government has given U.S. beef the go-ahead to enter the country — but that doesn't mean supermarkets are racing to stock up on American meat just yet. Japan's major supermarket chains expressed caution on Tuesday, December 13, a day after the country's U.S. beef ban was eased, wary of loading their shelves with American steaks Japanese consumers might not be ready to buy. "We have no plans to sell U.S. beef for now," said Aiichiro Yamaguchi, a spokesperson for Daiei Inc., one of Japan's largest chains. "We will listen to customers' opinions and see their reactions." Japan banned American beef imports in December 2003 after the first case of mad cow disease in the U.S. herd. After two years of negotiations and the lengthy Japanese approval process, Tokyo opened the doors to meat from U.S. cows aged 20 months or less. Other supermarket chains were also cautious. An official for Ito-Yokado Co., Japan's second-largest chain operator with 181 stores, said the chain has no immediate plans to sell U.S. beef until consumers feel confident about its safety.

Source: <http://www.cbsnews.com/stories/2005/12/13/ap/health/mainD8EFAT8O0.shtml>

[\[Return to top\]](#)

## **Water Sector**

18. *December 13, Associated Press* — **Governors to sign Great Lakes agreement.** Governors of the eight Great Lakes states are poised to sign an agreement Tuesday, December 13, aimed at preventing or minimizing the diversion of water from the lakes, the world's largest freshwater system. The governors, along with the premiers of two Canadian provinces sharing the Great Lakes, agreed more needed to be done to protect the water supply after a 1999 study of laws and policies protecting the lakes showed vulnerabilities. After five years of work and 10,000 public comments, the governors of Illinois, Indiana, Michigan, Minnesota, New York, Ohio, Pennsylvania, and Wisconsin have agreed on the protective compact. The agreement includes a ban on new diversions of water to areas outside the Great Lakes-St. Lawrence River Basin, with a limited number of exceptions. Communities and counties that straddle the basin line

could extract water from the lakes if they send back an equal amount of treated wastewater. The compact establishes a consistent standard that the Great Lakes states and provinces will use when reviewing proposed uses of lake water. It also requires the states and provinces to adopt conservation programs. Each state legislature would have to approve the agreement before Congress could enact a law enforceable in federal court.

Source: [http://www.gazetteextra.com/greatlakes\\_agreement121305.asp](http://www.gazetteextra.com/greatlakes_agreement121305.asp)

**19. *December 12, Associated Press* — Water officials: Las Vegas could outgrow Colorado River by 2007.**

The booming Las Vegas area's water demands could outstrip the region's share of the Colorado River by 2007, according to the 2006 water budget approved by the Southern Nevada Water Authority board this week. Kay Brothers, the Water Authority's deputy general manager, called that timeline a worst-case scenario, adding that through conservation and careful planning the state's share of the river water could be stretched beyond 2007. But Brothers acknowledged that the day is coming when southern Nevada will no longer be able to depend largely on its allotment from the river which currently supplies 90 percent of the area's drinking water. The water authority has had to come up with back-up resources, just in case. The 2006 water resource plan approved along with the agency's budget Thursday, December 8, outlines some of those options. They include about 290,000 acre-feet of groundwater stored beneath the Las Vegas Valley, 30,000 acre-feet banked with California, and an agreement with Arizona that guarantees Nevada 1.25 million acre-feet of water over the next 30 years. The water authority already has plans to build a two-billion-dollar pipeline to pump groundwater from rural basins in rural Nevada.

Source: <http://www.lasvegassun.com/sunbin/stories/nevada/2005/dec/09/120910421.html>

[\[Return to top\]](#)

## **Public Health Sector**

**20. *December 13, Reuters* — Indonesia confirms ninth death from bird flu.** Indonesia has confirmed its ninth human death from bird flu, senior Health Ministry officials said on Tuesday, December 13, taking the global death toll from the disease to 71, all in Asia. A Hong Kong laboratory affiliated with the World Health Organization confirmed an Indonesian had died from the H5N1 strain of bird flu. "We have received confirmation. (The death toll) is now nine," Hariadi Wibisono told Reuters about the findings on a 35-year-old man who died last month, making him the latest confirmed death in Indonesia, the world's fourth-most populous nation. Another senior health ministry official told Reuters the man lived in West Jakarta where he had contact with live chickens that carried the H5N1 virus. "He was building his house and around it there were many chickens and birds running around. Researchers tested those birds and they were positive" carriers of H5N1, said Nyoman Kandun, director general of disease control at the health ministry. Jakarta is preparing an early bird flu warning system aimed at reaching remote areas to speed up reporting of any outbreaks.

Source: <http://www.alertnet.org/thenews/newsdesk/JAK278190.htm>

**21. *December 13, Washington Post* — More scrutiny sought for reused devices.** A key member of Congress called Monday, December 12, for more rigorous federal oversight of reused medical devices designated as one-time-use instruments. The Food and Drug Administration (FDA) has made progress in monitoring the industry — called reprocessing — but "significant



gaps remain," said Rep. Rosa L. DeLauro (D-CT), the ranking Democrat on the House Appropriations subcommittee that oversees the FDA. Reprocessing is a growing industry that is believed to serve hospitals in all 50 states and the District of Columbia. Device manufacturers say they cannot vouch for the safety of their reconditioned single-use devices, but reproprocessors say there is no credible evidence that their refurbished devices are riskier than new ones. They also say no surgery is without risk, and many hospitals cite the practice's safety and cost savings. DeLauro, however, expressed concerns about the FDA's role. The agency relies on doctors to voluntarily report problems with faulty medical devices, and medical facilities are required to report to the FDA deaths but not device malfunctions. The FDA said that prior to 2000 it did little to oversee reproprocessors other than inspect their facilities and require them to follow good manufacturing practices. Now, it requires reproprocessors to submit data to validate that their work produces safe devices.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/12/AR2005121201469.html>

22. *December 13, Health-IT World* — **Computer models demo bird flu migration.** Computer simulation public health experts preparing for a feared avian flu pandemic are using computer models to get a glimpse of how the disease might spread if the bird virus were to start passing between people. The Models of Infectious Disease Agent Study (Midas) is funded by the National Institute of General Medical Sciences. Midas researchers in the U.S. and Britain are working along with other U.S. government agencies and the World Health Organization to outline how best to control a nascent flu epidemic. To model the avian flu, researchers used a cluster of 32 processors to simulate how 500,000 individuals in Thailand move and interact during a given period of time. The models simulate where each person is likely to go each day and how many people he or she will come in contact with. The data revealed that an outbreak could take off quickly and would be difficult to contain unless healthcare professionals and public health officials took action immediately. Now the researchers are using supercomputers to create a similar model for the much larger U.S. population.

Source: <http://www.health-itworld.com/newsletters/2005/12/06/16849>

23. *December 12, Associated Press* — **Blood donations refused over malaria.** Tens of thousands of would-be blood donors are turned away each year in case they picked up malaria while traveling abroad. Only a small portion of those people are thought to be infected. But the U.S. has no way to test donated blood for malaria. "This is an unmet need," said Jay Epstein, the Food and Drug Administration's (FDA) blood chief. Maintaining the blood supply is a balancing act. Some 34,000 pints are needed every day, and demand is rising annually. Yet only about five percent of the people eligible to donate blood do so, and scientists must guard the supply against a long list of infections. FDA rules require blood banks to ask would-be donors if they have lived in or traveled to a malaria-prone country, and postpone donations from those who answer yes in case the parasite is silently incubating in their bodies. Donations from short-term travelers are refused for one year; anyone who spent more than a year in a malaria-prone country or suffered malaria-like symptoms cannot donate for three years. From 2000 through 2004, the Red Cross lost 364,562 donations to malaria deferrals, Red Cross researcher Megan Nguyen told a meeting of the American Society of Tropical Medicine and Hygiene on Monday, December 12.

Source: [http://www.grandforks.com/mld/grandforks/living/health/13392\\_104.htm](http://www.grandforks.com/mld/grandforks/living/health/13392_104.htm)

## **Government Sector**

Nothing to report.

## **Emergency Services Sector**

**24. *December 13, Department of Homeland Security* — New Orleans Saints urge Americans to prepare for emergencies.** From their temporary home in San Antonio, TX, the New Orleans Saints football team spoke to Americans about the recent disaster that struck their hometown, and the importance of being prepared for such emergencies. Saints team members recorded a public service advertisement (PSA) that urges Americans to take some simple steps to prepare for emergencies. Following their November 18 practice, Saints Head Coach Jim Haslett, quarterback Aaron Brooks and wide receivers Joe Horn and Donte Stallworth discussed the devastation of Hurricane Katrina as a launching point to talk about emergency preparedness. Through a series of questions directed at the viewers, the Saints identify some of the most important steps individuals and families can take to be prepared. The PSA encourages viewers to visit Homeland Security's Ready campaign Website to learn more about these steps. The Saints PSA is the latest ad for Homeland Security's Ready campaign, one of the most successful campaigns in Ad Council history. To view the new PSA, which will be distributed to television stations nationwide this week via The FastChannel Network, visit the Ad Council Website.

Ad Council Website: <http://www.adcouncil.org/>

Department of Homeland Security's Ready campaign Website: <http://www.ready.gov/>

Source: <http://www.dhs.gov/dhspublic/display?content=5057>

**25. *December 12, Federal Computer Weekly* — Hawaii ready for storms, tsunamis.** National Weather Service (NWS) officials announced last week that Hawaii is the first state in the country to be prepared for severe weather storms and tsunamis under voluntary federal guidelines. Under the NWS programs, all four of the state's counties achieved the distinctions of StormReady and TsunamiReady, which the agency designed to help communities meet certain communications and safety guidelines and skills. Although the programs are separate, much of the criteria are similar. In both programs, communities must establish a 24-hour warning point to receive and disseminate NWS information and activate the local warning system. They must also have established emergency operations centers for jurisdictions that have more than 2,500 people. Those emergency operations centers and warning points must be able to receive and send weather information in multiple ways, including via National Oceanic and Atmospheric Administration (NOAA) Weather Radios, satellite downlink feeds from NWS, a statewide telecommunications network, amateur radio transceivers, wireless devices and local radios. To be ready for tsunamis, communities must also connect to NOAA's Weather Wire via the Internet, receive e-mail and pager messages from the Pacific Tsunami Warning Center, and monitor Coast Guard broadcasts, among other methods.

Source: <http://www.fcw.com/article91705-12-12-05-Web>

26. *December 12, National Journal's Technology Daily* — **Traditional communications systems reliable in disasters, panelists say.** Traditional modes of communication continue to serve as reliable, near-term solutions during emergencies, a panel of industry experts said Monday, December 12. Emergency responders are still served well by technologies they know, despite the development of technologies such as Internet telephony and satellite-based voice service, the experts said at the National Conference on Emergency Communications at George Washington University. "It all goes back to making do with what you have," said Dennis Wingo, the president of Assured Power and Communications. Wingo, who was part of the early relief effort in Jackson County, MS, following Hurricane Katrina in August, said problems with power supplies, terrestrial infrastructure, training and the ability of equipment to communicate across jurisdictions make emerging technologies less appealing for emergency personnel. He said cellular telephones and amateur radio remain the most reliable methods of interoperable technology. Oak Ridge Tech Connect's Eric Novotny said emergency responders typically will use technologies they know well. He said the best short-term strategy to better communications would involve making the networks that use those technologies as robust as possible.  
Source: [http://www.govexec.com/story\\_page.cfm?articleid=32997&dcn=to\\_daysnews](http://www.govexec.com/story_page.cfm?articleid=32997&dcn=to_daysnews)

[[Return to top](#)]

## **Information Technology and Telecommunications Sector**

27. *December 13, InfoWorld* — **Vodafone buys Telsim for \$4.5 billion.** Vodafone Group on Tuesday, December 13, said it plans to buy Turkish operator Telsim Mobil Telekomunikasyon Hizmetleri for \$4.5 billion. Telsim will require about \$1 billion of additional funding in the short term for investments in the operations and network of the operator, Vodafone said in a statement. Those investments are expected to result in losses for Telsim in the short to medium term. Vodafone sees opportunities in Turkey with mobile phone penetration at around 53 percent. Currently, Telsim has nine million customers, Vodafone said. The deal must be approved by Turkish government bodies and the board of Turkish Savings Deposit and Investment Fund, the current owners of Telsim. Vodafone expects the transaction to close in the first quarter next year.  
Source: [http://www.infoworld.com/article/05/12/13/HNvodafonebuystelsim\\_1.html](http://www.infoworld.com/article/05/12/13/HNvodafonebuystelsim_1.html)
28. *December 12, FrSIRT* — **Nortel SSL VPN Web interface remote command execution vulnerability.** A vulnerability has been identified in Milliscripts, which may be exploited by attackers to execute arbitrary commands. This is due to an input validation error in the "tunnelform.yaws" script when processing a specially crafted "a" parameter, which may be exploited by attackers to inject arbitrary commands via the embedded Java Applet and cause malicious scripting code to be executed by the user's browser in the security context of an affected Website. Solution: Upgrade to version 5.1.5.  
Source: <http://www.frsirt.com/english/advisories/2005/2845>
29. *December 12, InfoWorld* — **New attack targets known Mozilla bug.** Computer users who have not upgraded to the latest version of Mozilla Corp.'s Firefox browser may now have an extra incentive to do so, thanks to a hacker going by the name of Aviv Raff. On Sunday, December 11, Raff published a sample code  
<http://aviv.raffon.net/2005/12/11/MozillaUnderestimateVulne>

[rabilityYetAgainPlusOldVulnerabilityNewExploit.aspx](#)) that could be used to take over the computers of Firefox users running version 1.0.4 or earlier of the browser. The exploit takes advantage of a known bug (<http://www.mozilla.org/security/announce/mfsa2005-50.html>) in the way that Firefox processes the popular Javascript Web programming language. "I think it's been enough time for people to upgrade from v1.0.4. of Firefox. So, here is the PoC [proof of concept] exploit for the...vulnerability," he wrote on his blog. The bug was fixed in Mozilla version 1.0.5, which was released last July, and has also been fixed in version 1.7.9 of the Mozilla Suite, said Mike Schroepfer, vice president of engineering with Mozilla Corp. In some ways, this latest exploit is similar to the attack code that has been circulating for Microsoft's Internet Explorer browser, said Russ Cooper, scientist with security vendor Cybertrust Inc. "It can install and run code of the attacker's choice if a victim visits a malicious Website," he said. Source: [http://www.infoworld.com/article/05/12/12/HNmozillabug\\_1.htm](http://www.infoworld.com/article/05/12/12/HNmozillabug_1.htm)

30. *December 12, CNET News* — **New York City plans for Wi-Fi.** New York City lawmakers are taking a long, hard look at using 802.11-based Wi-Fi or some other technology to get the city's roughly eight million citizens access to broadband. New York's interest in municipal broadband comes just as the citywide Wi-Fi buzz hits a fever pitch. Other cities, such as Philadelphia, New Orleans and San Francisco, have already started down the Wi-Fi path, but if New York builds out its own Wi-Fi network, it will be the biggest deployment of municipal Wi-Fi in the country, and perhaps the world. "It's likely not a question of 'if' but 'when'," said Craig Mathias, an analyst with Farpoint Group of Ashland, MA. At this point New York is still in the very early stages of planning its broadband strategy. While cities like Philadelphia, New Orleans and San Francisco are moving full steam ahead on their projects, New York is still just trying to get a commission together to look at the issue. As with Philadelphia and San Francisco, New York officials want networks to be built that will bridge the digital divide so that even the city's poorest residents have affordable access to high-speed Internet connections. Source: [http://news.com.com/Can%20Wi-Fi%20make%20it%20in%20Manhattan/2100-7351\\_3-5992316.html?tag=nefd.top](http://news.com.com/Can%20Wi-Fi%20make%20it%20in%20Manhattan/2100-7351_3-5992316.html?tag=nefd.top)

31. *December 12, PC Pro (United Kingdom)* — **Researchers crack biometric security with Play-Doh.** Using fake fingerprints, researchers in New York have managed to break nearly all the biometric identification systems they tested. Headed by Clarkson University associate professor of Electrical and Computer Engineering Stephanie C. Schuckers, they used fake fingers made by taking casts of live fingers and using the molds to create copies in Play-Doh. The 60 fake fingers were then tested and were successfully authenticated by the combination of the fingerprint readers and their accompanying software in nine out of every ten attempts. "Digits from cadavers and fake fingers molded from plastic, or even something as simple as Play-Doh or gelatin, can potentially be misread as authentic," Schuckers explained. The team subsequently developed a technique for distinguishing live digits by detecting changing moisture patterns and reduced the false detection rate to less than 10 percent. "Since liveness detection is based on the recognition of physiological activities as signs of life, we hypothesized that fingerprint images from live fingers would show a specific changing moisture pattern due to perspiration but cadaver and spoof fingerprint images would not," Schuckers explained. Source: <http://www.pcpro.co.uk/news/81257/researchers-crack-biometric-security-with-playdoh.html>

## Internet Alert Dashboard

### DHS/US–CERT Watch Synopsis

**Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.**

**US–CERT Operations Center Synopsis:** US–CERT is aware of a cross domain violation in Internet Explorer. This may allow a script in one domain to access web content in a different domain. Web browsers should adhere to the "Same Origin Policy", which prevents documents or scripts loaded from one origin from getting or setting properties of a document from a different origin. Internet Explorer does not follow this policy when importing CSS documents. For more information please see URL: <http://www.mozilla.org/projects/security/components/same-origin.html>

If the cross domain violation in Internet Explorer occurs on a system that has Google Desktop Search (GDS) installed, then an attacker may be able to search for private data, execute programs, or execute arbitrary code on this vulnerable system. Google has modified its web pages to prevent exploitation of GDS through this particular vulnerability in Internet Explorer. The cross domain violation vulnerability in Internet Explorer is still present, however. Although there is limited information concerning this vulnerability, US–CERT encourages users to disable Active scripting to prevent exploitation. For more information please review URL:

[http://www.cert.org/tech\\_tips/malicious\\_code\\_FAQ.html#ie566](http://www.cert.org/tech_tips/malicious_code_FAQ.html#ie566)

Users can also refer to the Microsoft Security Response Center Blog for some additional information on this vulnerability affecting Internet Explorer. For more information please see:

<http://blogs.technet.com/msrc/archive/2005/12/07/415740.aspx>

US–CERT has observed increased traffic affecting port 53 since the release of W32.Spybot.ABDO. Symantec's write up points out that Spybot.ABDO opens a back door by connecting to an IRC server through TCP port 53. Looking at the Port 53 Report using DShield data, shows that the number of targets has more than doubled in the past 48 hours. Other malware that has been discovered in recent months, using Port 53, include Backdoor.Civcat, Trojan.Esteems.C, Trojan.Esteems, and W32.Beagle.BH@mm. For more please see the following URL:

<http://isc.sans.org/diary.php?storyid=928>

### Current Port Attacks

<b>Top 10 Target Ports</b>	1026 (win-rpc), 6881 (bittorrent), 445 (microsoft-ds), 80 (www), 4142 (oidocsvc), 25 (smtp), 135 (epmap), 139 (netbios-ssn), 6346 (gnutella-svc), 32789 (---) Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center
----------------------------	--

To report cyber infrastructure incidents or to request information, please contact US–CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://www.us-cert.gov).

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.



## **Commercial Facilities/Real Estate, Monument & Icons Sector**

- 32. *December 13, The Express–Times (PA)* — Pennsylvania school gets second bomb threat in week.** Students and staff were evacuated from Shawnee Middle School in Easton, PA, for the second time in less than a week on Monday morning, December 12, when the school received two phone calls indicating a bomb was in the building. Principal Stephen Furst said the calls came in between 7:45 a.m. and 8:05 a.m. EST, but he would not name exact times, citing security reasons. Students were evacuated from the building and moved off the campus. After a bomb threat Thursday morning, December 8, students and staff were taken to Paxinosa Elementary School while officials and a bomb–sniffing dog secured the premises. Furst would not say if the threats were the same as last week's, nor would he say if the calls had been taped. The Easton Area School District and the district's police department are investigating the threats.

Source: <http://www.nj.com/news/expresstimes/pa/index.ssf?/base/news-3/1134468343223660.xml&coll=2>

- 33. *December 13, The Selma Times–Journal (AL)* — Alabama school officials to get safety training.** Dallas County, AL, school personnel will undergo awareness training for suspicious devices from the Montgomery Police Department and the Alabama Bureau of Investigation (ABI) in January. The training will come in handy after a suspicious package was discovered in Southside High School on Thursday, December 8. The Montgomery Police Department bomb squad, the ABI, and the Bureau of Alcohol, Tobacco and Firearms and Explosives investigated and rendered the package safe. The police department says it has received several school bomb threats over the past two months, all of which have been made using pre–paid cell phones. Dallas County School Superintendent Fannie Major–McKenzie said the January training session will focus on the procedures already in place within the school system and enhancing them.

Source: <http://www.selmatimesjournal.com/articles/2005/12/13/news/local/news2322.txt>

- 34. *December 12, The Daily Star (NY)* — New York City agrees to begin work on dam.** Progress is being made on efforts to avert a possible crisis at the Gilboa Dam, part of the New York watershed. The structure has been the subject of concern since engineers determined in September that the dam could fail under a rare set of circumstances. Structural repairs were planned for spring with rebuilding scheduled for 2010. According to New York City Department of Environmental Protection spokesperson Ian Michaels, the repairs could begin sooner than planned. He said, "This should be our top priority. We should do everything possible to get it fixed as soon as possible." To do this, the dam is being drained as fast as possible to bring water levels down to allow the work to begin and take pressure off the structure. Siphon drains are scheduled to be built in January, Michaels said. Also in January, a 200–foot wide, five– to six–foot–deep notch will be cut out at the top of the dam wall to keep water levels down, among other things. The final design will include flood control provisions, as recommended by the Army Corps of Engineers. Approximately 5,000 people live in the area affected.

Source: <http://www.thedailystar.com/news/stories/2005/12/12/gdw5.htm1>

**35. *December 12, Associated Press* — South Carolina educator's plan would put cameras in the classroom.** Education Superintendent candidate Karen Floyd said Monday, December 12, she wants to expand video surveillance in South Carolina's schools as part of her plan to address school violence. She said she is not proposing putting cameras in every classroom, but targeting areas most at-risk. Some school districts said they are already using video surveillance, but the equipment is in common areas and on buses, not individual classrooms. Horry County School District spokesperson Teal Britton said surveillance cameras in common areas, like hallways and building perimeters, have been the standard there "for years...Security is something that has to be a building principal's priority at any given time." Britton also said Horry County employs a full-time canine drug team, which conducts random, unannounced visits. Security officials also use handheld metal detectors and breathalyzers when needed, she said. The story was the same in the Charleston County School District, where spokesperson Jerry Adams said cameras are used in common areas but not in individual classrooms.

Source: <http://www.myrtlebeachonline.com/mld/myrtlebeachonline/news/local/13391285.htm>

[\[Return to top\]](#)

## **General Sector**

Nothing to report.

[\[Return to top\]](#)

### **DHS Daily Open Source Infrastructure Report Contact Information**

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

### **DHS Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:	Send mail to <a href="mailto:dhsdailyadmin@mail.dhs.osis.gov">dhsdailyadmin@mail.dhs.osis.gov</a> or contact the DHS Daily Report Team at (703) 983-3644.
Subscription and Distribution Information:	Send mail to <a href="mailto:dhsdailyadmin@mail.dhs.osis.gov">dhsdailyadmin@mail.dhs.osis.gov</a> or contact the DHS Daily Report Team at (703) 983-3644 for more information.

### **Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright

restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.